STATEMENT OF RACHEL NOSOWSKY, ESQ.
Assistant General Counsel, University of Michigan
Member, caBIG™ Data Sharing and Intellectual Capital Workspace

American Health Information Community (AHIC)
Confidentiality, Privacy and Security Workgroup Meeting

June 22, 2007

Thank you for the opportunity to present to you today about caBIG™, the National Cancer Institute's Cancer Biomedical Informatics Grid™. My name is Rachel Nosowsky. I serve as Assistant General Counsel at the University of Michigan, where I advise institutional review boards and researchers about legal and regulatory requirements for conducting human research and protecting individual privacy. I also serve as a member of caBIG's Data Sharing and Intellectual Capital (DSIC) Workspace, a workgroup involved in the development and support of caBIG. In addition to my caBIG colleagues who have come here today – Ken Buetow and Wendy Patterson at NCI, and Marsha Young at Booz Allen Hamilton, I would like to acknowledge the tremendous contributions to DSIC of Deborah Collyar, President of Patient Advocates in Research (PAIR), who was unable to attend today's meeting. Deb has been a leading and tireless voice in the DSIC Workspace, advocating for acceleration of scientific discovery and medical progress in a manner that protects the privacy and autonomy interests of patients and research participants.

caBIG™ BACKGROUND

The National Cancer Institute (NCI) is charged by Congress through the National Cancer Act to lead the nation's cancer research efforts. NCI's mission is to reduce the burden and eliminate the adverse outcomes of cancer by leading an integrated effort to advance fundamental knowledge about cancer across a dynamic continuum of discovery, development, and delivery.[1]
In service of this mission, the NCI seeks to utilize the insights of molecularly targeted or "personalized" medicine – the use of a patient's detailed genomic information and clinical data to drive selection of a medication, therapy or preventive measure that is particularly suited to that patient at the time of administration[2-4] – to improve patient outcomes.

The NCI's senior leadership has recognized that barriers to access to and use of information technology (IT) is a critical and early stumbling block to leveraging the benefits[5] of personalized medicine. In response, the NCI has established the strategic goal of utilizing biomedical informatics to create a virtual web of interconnecting data, individuals, and organizations to redefine how biomedical research is conducted, clinical care is provided, and patients interact with the biomedical research enterprise. To achieve this objective, NCI launched the caBIG initiative in February 2004. NCI's intent is to create a standards-based distributed informatics infrastructure – bridging individual institutional and organizational silos in the broader cancer research community – to facilitate the sharing of data and research findings. caBIG's vision is "a full cycle of integrated cancer research, extending from bench to bedside, and back again."[6]

The developing caBIG infrastructure[7] utilizes community-defined standards and architecture to support interoperable software applications and enable the sharing of cancer data. This infrastructure leverages existing resources and supplements these with new applications, toolkits, and other devices developed by experts in the caBIG community to:

- provide scientists with the ability to collaborate and integrate data and findings to accelerate research;
- assist the cancer community with priority setting, decision-making, and participation to accelerate completion of clinical trials
- empower advocacy groups and individual patients to participate in clinical research; and
- help healthcare providers become patients' partners in the research enterprise and educated consumers of research findings.

All products created with NCI caBIG program funds are made available on an open development, open source and open access basis.

The caBIG infrastructure is designed to promote personalized medicine by creating the capacity to integrate and aggregate information that has been collected at different times, in different locations, by different clinical and research groups. Thus, for example, a researcher involved in a phase II clinical trial of a new targeted therapeutic for brain tumors might observe that cancers derived from one specific tissue progenitor appear to be strongly affected. If the trial has been generating proteomic and microarray data, the researcher might use caBIG products to identify potential biochemical and signaling pathways that might be different between this cell type and other potential progenitors in cancer, deduce whether anything similar has been observed in other clinical trials involving agents known to affect these specific pathways, and identify any studies in model organisms involving tissues with similar pathway activity. By utilizing the caBIG infrastructure, researchers at individual institutions can connect to data and resources in a way that was never before possible – catalyzing discovery and facilitating the practice of oncology specifically, and of medicine in general.

caBIG™ AND THE DATA SHARING AND INTELLECTUAL CAPITAL WORKSPACE

The caBIG community convenes through numerous teleconferences and face-to-face meetings, which are open and available to anyone who chooses to participate. Participants are drawn from academic institutions, industry, standards development organizations, advocacy groups, government sponsors and regulatory agencies. They are organized through various Workspaces, which in turn identify and execute caBIG priorities:

- *Domain Workspaces* focus on informatics problems in a particular domain of cancer research – clinical trials, imaging, tissue banks, genomics, proteomics, epidemiology and population sciences.

- *Cross-Cutting Workspaces* integrate the Domain Workspaces together into a common framework with consistent architecture and standards.

- *Strategic Workspaces* address issues of concern to both the Domain and Cross-Cutting Workspaces and set the overall guidelines and goals for the caBIG program.

The Data Sharing and Intellectual Capital (DSIC) Workspace is a strategic level caBIG Workspace whose members include biomedical researchers, clinicians, technology transfer experts, intellectual property and regulatory attorneys, policy specialists, patient advocates, bioethicists, and bioinformaticists. They participate in workspace-wide activities and through two individual Special Interest Groups (SIGs): one that focuses on regulatory issues and another that focuses on intellectual property and proprietary concerns.

CHALLENGES FOR THE caBIG™ COMMUNITY

caBIG participants represent a broad range of organizations including health care providers and researchers, patients and research participants, public and private sponsors, application developers, and more. The diversity of this community creates substantial challenges to data sharing. Among the barriers identified by DSIC:

- caBIG participants have varying obligations under federal and state data privacy[8] and security[9] laws and standards, including the Health Insurance Portability and Accountability Act of 1996[10] and associated privacy and security rules (collectively "HIPAA"),[11] FDA security regulations,[12] and FISMA.[13]

- Human research is subject to oversight by a broad range of ethical review boards – IRBs – whose local requirements regarding collection, maintenance, and use of identifiable data often vary substantially based in part on the requirements of the Common Rule,[14] FDA regulations,[15] and other federal, state, and voluntary regulations, standards and codes.

- Academic considerations (the need to secure grants and publish research results in peer-reviewed literature) often discourage sharing, particularly during early stages of research.

- Researcher and sponsor concerns regarding ownership and control of intellectual property are substantial; industry funding and material transfer agreements often require at least temporal restrictions on data sharing.

- Safety concerns related to premature access to unvalidated information discourage researchers who otherwise might be inclined to share data from doing so.

- Public perceptions regarding privacy, security and confidentiality of health information, informed at least in part by widespread distrust of electronic data storage and of the human research enterprise more broadly, make it difficult for researchers and research institutions to champion data sharing initiatives.

DSIC's mission is to facilitate data sharing between and among caBIG participants by addressing these legal, regulatory, ethical, policy, academic, proprietary and contractual barriers to data exchange for public health and research purposes. Our members believe that strong confidentiality, privacy and security measures are both necessary and feasible in any electronic health information exchange (eHIE) environment and that they can be scaled to accommodate a broad range of participants, without unnecessarily impeding scientific discovery and medical progress.

REMOVING BARRIERS TO DATA SHARING

The caBIG™ community has, from the start, anticipated the need to accommodate diverse stakeholders' varying needs for data confidentiality, privacy and security standards and assurances, and continues to work to eliminate or reduce identified barriers to the broad data sharing that is necessary to advance scientific progress and speed medical discovery. caBIG's efforts have focused in three areas: a federated architecture for data sharing – to maintain local control of clinical and research records; an analytical framework designed to encourage consistent analysis of legal, regulatory, ethical and other barriers to data sharing and identify solutions; and standards, tools and infrastructure broadly available to members of the caBIG community and beyond to facilitate data sharing.

Federated Architecture

The technical infrastructure of the caBIG™ program is based on a set of technologies called caGrid. This infrastructure is designed as a web-services, standards-based, federated biomedical information network that allows systems constructed according to a series of compatibility guidelines[16] to interoperate with each other, and with properly authorized and authenticated end users. Like its overall architecture, the security infrastructure of caGrid is federated, allowing users to authenticate (assert their identity) at their local institutions, while allowing data providers to retain local control of the decision to authorize access to any particular data resource. This process is implemented through a combination of technology and trust agreements between the entity managing a specific instance of the caGrid infrastructure and local data and identity providers, which can be enforced through a combination of laws, regulations, formal contractual commitments and informal terms of use.

The caBIG instance of the caGrid infrastructure is known as 'NCI-caGrid.' The federated, distributed nature of caGrid technology also allows for the creation of a series of caGrid-connected networks that are managed independently but are interoperable with the NCI-caGrid. This flexibility allows an individual medical center, cooperative group, or other entity to set up its own instance of caGrid that can operate behind a firewall, or with different security requirements than the NCI-caGrid's. However, a local caGrid can interact with the NCI-caGrid so long as an appropriate trust agreement is implemented. Similarly, the NCI-caGrid can interact with other large-scale implementations of caGrid technology that are expected to be compatible with caBIG, such as the upcoming CardioVascular Research Grid (CVRG) or the United Kingdom's National Cancer Research Institute (NCRI ONIX).

Strategic Implementation: Analytical Framework

DSIC recognizes that different data require different types of protection. Some data, such as individually identifiable human health information, are highly sensitive and require significant protection to address legal, regulatory and ethical constraints on access and use. Other data, for example, highly aggregated or completely deidentified data sets, typically do not require such protection. To address these differences and facilitate data sharing within the caBIG™ community, DSIC has developed a framework (see Attachment 1) that we believe can be helpful to analyzing challenges and identifying opportunities for the caBIG community and to electronic health information exchange (eHIE) initiatives more generally.

The framework is designed to empower and encourage individuals and institutions seeking to share data to consistently analyze any constraints on such efforts, grouped into four broad categories: (i) economic or proprietary concerns of researchers and research institutions; (ii) federal and state privacy and security laws and regulations and institutional policies; (iii) ethical considerations, reflected in explicit consumer- and institutional review board (IRB)-imposed constraints on data sharing, including restrictions specified in informed consent documents; and (iv) contractual restrictions imposed by research sponsors. Once identified, DSIC believes that many of those barriers can be reduced or even eliminated, at least for some subsets of data. These objectives are being accomplished through the series of existing and planned standards, tools, and infrastructure arrangements described below.

Technical Implementation: Standards, Tools, and Infrastructure

DSIC and other caBIG™ Workspaces are developing and implementing standards, tools and infrastructure to support data sharing consistent with the constraints described above. For example, to complement the framework described above, DSIC is developing:

- Web-based terms of use and standardized contractual provisions for trust agreements designed to facilitate data sharing consistent with HIPAA and other applicable federal and state privacy and security laws and with human research protection regulations and accreditation standards.

- Model language for applications submitted to IRBs designed to educate their members regarding the caBIG and the NCI-caGrid, the benefits and risks of data sharing, and various mechanisms available to mitigate risks and utilized in various caBIG tools.

- Model language for informed consent and authorization documents, designed to encourage consumers to participate in the caBIG initiative, consistent with legal and regulatory requirements specified in the Common Rule, FDA regulations, accreditation standards, and HIPAA.

caBIG's Tissue Banks and Pathology Tools (TBPT) Workspace has developed caTISSUE Core, a tool designed to track the extent to which individual patients or research participants have given permission for their collected biospecimens and related data to be used for research purposes. These permissions frequently are granted during the course of a patient encounter or

clinical trial. This tool allows users to track different tiers of consent as well as decisions by research participants to withdraw consent for the use of specific specimens. The primary drivers for this tool are the need to fulfill ethical obligations to patients and research subjects to honor their expressed wishes, and the desire to reduce ambiguity with respect to the ability to utilize biosepcimens for translational research. Other tools being deployed to support other components of the clinical research endeavor include caExchange, under development by the Clinical Trials Management Systems (CTMS) Workspace, the National Cancer Imaging Archive, implemented by the In Vivo Imaging (IMAG) Workspace, and caArray, produced through the Integrative Cancer Research (ICR) Workspace.

Finally, the NCI-caGrid Security Working Group (SWG) develops and recommends security policies and procedures for sharing data via the caGrid technology stack. DSIC provides support to the SWG on security policy matters. Primary responsibility for security implementation for the NCI-caGrid is the NCI, which will review SWG recommendations to verify that they are not in conflict with federal law or regulations. Areas where the SWG will offer recommendations include:

- periodic security risk assessment procedures for caGrid infrastructure and portions of NCI-caGrid-facing services or components;
- security policies regarding federated authentication, certificate management/provisioning, group-based authorization, protection of sensitive data, user security policies and procedures; and
- security policy implementation procedures for use in NCI-caGrid-facing components across caBIG.

In the near term, the SWG will create a set of baseline policies that will allow a low barrier to entry of data via the NCI-caGrid, particularly for systems that carry non-sensitive information. The SWG then will develop a set of policies and procedures sufficient for an entity with highly sensitive data to confidently permit access to those data through the NCI-caGrid. Such confidence can be achieved *only* if these policies and procedures are created through an open process that seeks input from all members of the diverse caBIG community; the SWG/DSIC system described above assures such a process.

DSIC RESPONSE TO AHIC CONFIDENTIALITY, PRIVACY & SECURITY WORKGROUP WORKING HYPOTHESIS

Our response to the Working Hypothesis starts from the premise that research is an essential component of the health care delivery system. "Central to the ability to deliver safe, effective, and patient-centered care is a need for better and timelier evidence on which to base clinical decisions about which medical interventions are best, for whom, and under what circumstances."[17] Indeed, in some settings, clinical care is delivered primarily through clinical trials. For example, most children with cancer receive their treatment at pediatric cancer centers; survival rates have increased dramatically in the past generation as a result.[18]

Relevant Standards

DSIC members understand that eHIE initiatives will succeed only if and to the extent participants can reassure consumers that their health information will be adequately and appropriately protected. Accordingly, we agree with the primary principle articulated in the Working Hypothesis, *i.e.*, that all participants in a health information exchange network (HIEN) must be expected to meet minimum privacy and security standards *such as* those reflected in the HIPAA privacy and security regulations, and that these standards must be enforceable. We also agree that some HIPAA standards and implementation specifications are less relevant to some HIEN participants than others. Indeed, we believe these standards unnecessarily impede research conducted by covered *and* non-covered entities, without any corresponding benefit to patient privacy or autonomy.

<u>Recommendation</u>: HIENs should not extend the following administrative restrictions and mandates on non-consumer research participants not otherwise subject to HIPAA:

- *Prohibition on Authorization for "Unspecified" Future Research*. To assure that individuals whose health information is protected by HIPAA are empowered to make informed choices about the use of that information, HIPAA requires as a central provision of any valid authorization a description of the specific planned purpose of the requested use or disclosure. The regulation thus prohibits "blanket authorizations" or permission for unspecified future research. Long before promulgation of the HIPAA Privacy Rule, however, the National Cancer Institute, together with the National Action Plan on Breast Cancer, developed and tested a model informed consent document and patient information brochure to facilitate collection and use of tissue specimens for research.[19, 20] The model form, which was developed with input from a diverse group of bioethicists, researchers, patient advocates, and others, permitted individuals participating in research studies to: (i) allow use of their excess tissues for cancer research; (ii) allow use of their excess tissues for any biomedical research; or (iii) be contacted in the future about other research opportunities. HIPAA prohibits such blanket authorization. To address the obvious impact on data and specimen research, HIPAA allows individuals to agree to the inclusion of their information in a research registry but requires that researchers obtain separate IRB or Privacy Board approvals and authorizations (or waivers) for each subsequent use of the registry. This arguably mitigates the effects of the problematic ban but it imposes an administrative burden on an already overburdened and underfunded oversight system that does nothing to substantively advance individual privacy or autonomy.

  <u>Recommendation</u>: Do not extend HIPAA's prohibition on blanket authorizations to researchers not covered by HIPAA. Consider alternative mechanisms[21] to permit consumers to make informed choices about the use of their health information for research.

- *Business Associate Requirements*. HIPAA's standards and implementation specifications require covered entities that wish to disclose individually identifiable health information to vendors and others to enter into "business associate agreements" with those third parties, thus essentially extending HIPAA's requirements to otherwise non-covered individuals and organizations by contract. HIPAA explicitly does not require covered entities to enter into business associate agreements with researchers. Rather, the regulation requires covered entities to disclose individually identifiable health information to researchers only under specified circumstances, generally with specific written authorization or under a waiver of authorization granted by an IRB or Privacy Board. Business associate contract requirements are difficult to implement and often offer no added protection to covered health information. For example, a covered entity that also functions as a business associate is required to comply with HIPAA regardless of its execution of a business associate agreement. Similarly, a covered entity should not be required to execute a business associate agreement with a researcher obligated through a written or electronic trust agreement to adhere to substantively similar privacy standards

  <u>Recommendation</u>: Do not require researchers accessing HIEN data to execute business associate agreements. Instead, include assurances regarding appropriate use and safeguards within standard HIEN trust agreements or terms of use.

- *Notices of Privacy Practices (NPPs)*. HIPAA requires that covered health care providers and health plans inform individuals seeking health care or coverage about their privacy practices upon a first encounter with a covered entity and at least once every three years thereafter. Moreover, industry standards require internet sites to maintain web privacy statements and similar notifications.[22, 23] The fact that HIPAA does not extend its notice requirement to health care clearinghouses does not justify a lower standard that deprives consumers of their ability to make informed decisions regarding participation. That said, some of HIPAA's NPP implementation specifications are not relevant in an eHIE environment.

  <u>Recommendation</u>: Require HIENs and their non-consumer participants to conspicuously post on publicly-available websites information about their privacy practices and security measures implemented to maintain the confidentiality of sensitive data.

  <u>Recommendation</u>: Do not require entities not covered by HIPAA to distribute paper copies of their notices to consumer participants; nor to secure written acknowledgement of receipt.

Enforcement

At base, eHIE standards may be enforceable through one or more of the mechanisms described in the following table:

Description	Enforcement Authority	Sanctions
Statute/Regulation - HIPAA - State genetics privacy laws - Etc.	- Government Agency - Prosecutor	- Warnings/reprimands - Use/access suspension or termination - Civil penalties - Criminal penalties
Common Law	- HIEN Organization - Private Litigators * Consumer Participants * Other HIEN Participants	- Use/access suspension or termination - Injunction - Money damages
Contract/Trust Agreement/ Terms of Use - Electronic or Written - Formal or Informal	- HIEN Organization - Other HIEN Participants - Consumer Participants (as "third-party beneficiaries")	- Use/access suspension or termination - Injunction - Money damages

It is unnecessary to impose HIPAA standards – and particularly HIPAA implementation specifications – on non-consumer HIEN participants who are not already covered by the regulation. HIENs have alternative means to adopt and enforce standards that assure privacy protection and consumer confidence.

<u>Recommendation</u>: Rely on trust agreements or other contractual solutions[24] for enforcement. If legislative or regulatory action is pursued to assure adherence of non-covered entities to specified confidentiality, privacy and security policies and procedures, assure it does not undermine existing accommodations for the research enterprise.

Minimum Standards

All eHIE participants must agree or otherwise be held to minimum standards or terms of use that assure appropriate and secure treatment of sensitive information. Failure to assure adherence to such standards will result in loss of confidence in a network by participants and, ultimately, its failure.

HIPAA applies to most health care providers and payors and, therefore, seems like a natural starting point for developing those standards. Yet even one of the regulation's primary authors acknowledges that, when initially drafted, HIPAA "was not a regulation about research. Research was not a central consideration, nor the thing that got the most attention, and it was also a difficult issue. . . . So, as a more difficult conversation that was not central to the policy debate, it was put off until late in the process. In the end, research did get a fair amount of attention, although not from people who were intimately familiar with how the research world operated."[25] Unsurprisingly, HIPAA suffers well-documented shortcomings that impede medical progress without significantly advancing individual privacy or autonomy.[26-28] Thus, notwithstanding widespread commitment by researchers to respecting study participants' privacy and securing the confidentiality of their data, there is little appetite within the research community to extend HIPAA's detailed requirements on those who are not legally required to comply with the rule and, in particular, some of its onerous implementation specifications.

A federated architecture such as the one adopted by the caBIG community is one mechanism HIENs can use to assure that all participants adhere to any existing legal obligations, ethical

standards and local practices. It works by permitting any contributor of data to limit access by others consistent with specified requirements. Thus, for example, a HIPAA-regulated health care provider might make available through the NCI-caGrid to the broader caBIG community only data that have been completely de-identified. That same provider might be willing to share identifiable extracts of the same dataset with a collaborator at another institution (typically through a locally operated caGrid) if the collaborator has agreed to certain assurances, either through standardized trust agreements or less formal click-through terms of use that meet applicable regulatory requirements (e.g., data use agreement assurances), or through non-standard bilateral written agreements.

Recommendation: It is unnecessary to extend the regulatory requirements of HIPAA to organizations receiving identifiable health information that are not "covered entities" under the existing rule. However, if HIPAA standards are to be more broadly imposed (whether by regulation, policy, or contract), treat research involving use or disclosure of eHIE data as a central "health care operation" to eliminate some of the burdensome administrative requirements of HIPAA without sacrificing important privacy protections. To assure ethical use of those data and conduct of studies (e.g., consistent with an individual's informed consent and authorization), permit such preferential treatment of research uses and disclosures only for activities that are approved by and subject to the oversight of a registered institutional review board (IRB) operating under a Federalwide Assurance.

Recommendation: Any revisions to HIPAA (or adoption of HIPAA-like standards) should, at a minimum, maintain any existing accommodations for research to avoid unintended but seriously negative impact on national, state and local research and public health activities.

CONCLUSION

Personalized medicine offers the opportunity to identify and apply evidence-based standards in real time, thereby improving our ability to deliver effective prevention and treatment to patients fighting cancer. Personalized medicine cannot exist apart from research. eHIE initiatives offer the research community the ability to leverage existing data both to expedite medical discovery and to optimize individual patients' care. We encourage AHIC and other stakeholders to enhance, not further limit, our ability to effectively conduct research while protecting individual patients' privacy and respecting their autonomy.

ACKNOWLEDGMENTS

I would like to acknowledge the invaluable contributions of the following individuals for helping me to shape the ideas and opinions described in my testimony and for preparing my materials: Ken Buetow, Ph.D., NCI; Wendy Patterson, J.D., NCI; George Komatsoulis, Ph.D., NCI, Patricia Weeks, B.S., Fox Chase Cancer Center; Marsha Young, J.D., Booz Allen Hamilton; Deborah Collyar, B.A., Patient Advocates in Research; Elaine Brock, J.D., M.H.S.A., University of Michigan; and Margia Corner, B.A., University of Michigan.

ENDNOTES

1. Von Eschenbach AC. The NCI Strategic Plan for Leading the Nation to Eliminate the Suffering and Death Due to Cancer. Washington, DC: National Cancer Institute; 2006.

2. Meadows M. Genomics and Personalized Medicine. FDA Consumer Magazine 2005;39(6).

3. Personalized Medicine. Wikipedia, 2007. (Accessed June 17, 2007, at http://en.wikipedia.org/wiki/Personalized_medicine.)

4. HHS Secretary Leavitt Announces Steps Toward a Future of "Personalized Health Care". 2007. (Accessed June 20, 2007, at http://www.hhs.gov/news/press/2007pres/03/pr20070323b.html.)

5. Muller AJ, Scherle PA. Targeting the mechanisms of tumoral immune tolerance with small-molecule inhibitors. Nat Rev Cancer 2006;6(8):613-25.

6. About caBIG(tm). National Institutes of Health, 2007. (Accessed June 17, 2007, at https://cabig.nci.nih.gov/overview.)

7. caBIG(tm) Overview. McLean, VA: MITRE Corporation; 2006 May 2006.

8. Health Privacy. National Conference of State Legislators, 2007. (Accessed June 17, 2007, at http://www.ncsl.org/programs/lis/privacy/medprivacy.htm.)

9. State Laws Governing Security Breach Notification. Crowell & Moring, 2007. (Accessed June 17, 2007, at http://www.crowell.com/pdf/SecurityBreachTable.pdf.)

10. Health Insurance Portability and Accountability Act. 42 US Code § 1320d; 1996.

11. U.S. Department of Health and Human Services. Standards for Privacy of Individually Identifiable Health Information and Security Standards for the Protection of Electronic Protected Health Information (HIPAA Privacy and Security Rules). 45 C.F.R. Parts 160 and 164; 2003.

12. U.S. Food and Drug Administration. Electronic Records; Electronic Signatures. 21 C.F.R. Part 11; 2004.

13. Federal Information Security Management Act of 2002. 44 USC §§ 3501-3549; 2002.

14. U.S. Department of Health and Human Services: Office for Human Research Protections. Basic HHS Policy for Protection of Human Research Subjects. 45 C.F.R. Part 46 Subpart A; 2005.

15. U.S. Food and Drug Administration. Informed Consent of Human Subjects. 21 C.F.R. Part 50 Subpart B; 2006.

16. caBIG(tm). The Cancer Biomedical Informatics Grid(tm) Program: caBIG(tm) Compatibility Guidelines; 2005.

17. Roundtable on Evidence-Based Medicine. Institute of Medicine, 2007. (Accessed June 20, 2007, at http://www.iom.edu/CMS/28312/RT-EBM.aspx.)

18. Care for Children and Adolescents With Cancer: Questions and Answers. National Cancer Institute, 2005. (Accessed June 20, 2007, at http://www.cancer.gov/cancertopics/factsheet/NCI/children-adolescents.)

19. National Action Plan on Breast Cancer: National Biological Resources Banks Working Group. Sunset Report; 1998.

20. National Action Plan on Breast Cancer Tissue Banking Working Group, PRIM&R/ARENA Tissue Banking Working Group. Model Consent Forms & Related Information on Tissue Banking from Routine Biopsies; 1998.

21. Kohane IS, Mandl KD, Taylor PL, Holm IA, Nigrin DJ, Kunkel LM. MEDICINE: Reestablishing the Researcher-Patient Compact. Science 2007;316(5826):836-7.

22. Guidelines for medical and health information sites on the Internet: Principles governing AMA Web sites. American Medical Association, 2000. (Accessed at http://www.ama-assn.org/ama/pub/category/1905.html.)

23. Your Online Privacy Policy: An informational paper about drafting your first privacy statement or improving your existing one. TRUSTe, 2004. (Accessed June 20, 2007, at http://www.truste.org/pdf/WriteAGreatPrivacyPolicy.pdf.)

24. Markle Foundation. The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange. New York; 2006.

25. Herdman R, Moses H. Effect of the HIPAA Privacy Rule on Health Research: Proceedings of a Workshop Presented to the National Cancer Policy Forum. 2006; Washington, DC: Institute of Medicine of the National Academies; 2006.

26. Aronovitz LG. Health Information: First-Year Experiences under the Federal Privacy Rule. Government Accountability Office; 2004.

27. Nosowsky R, Giordano TJ. THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA) PRIVACY RULE: Implications for Clinical Research. Annual Review of Medicine 2006;57(1):575-90.

28. Ness RB. A year is a terrible thing to waste: early experience with HIPAA. Annals of Epidemiology 2005;15(2):85-6.